FACTORISATION OF $X^n - \alpha$ OVER FINITE FIELDS - II

ABSTRACT. In this note, we are studying factorization in finite fields of polynomials $X^n - \gamma$ with factors grouping irreducible polynomials of same order. We describe a method of calcul of these factors by induction.

1. INTRODUCTION

In the previous note [1] is studied factorization of polynomials $X^n - \gamma$ into product of irreducible polynomials in $\mathbb{F}_p[X]$. We have seen that the polynomials $X^n - \gamma$ with γ going through all d-th primitive roots, all have the same distribution of orders for their irreducible factors, and that the orders k present in this factorization are the integers of the set $F_{n,d} = \text{Div}(nd) \setminus \bigcup_{l|d,\ l\neq d} \text{Div}(nl)$ where $\text{Div}(q)$ denotes the divisors of q. So we have $X^n - \gamma = \prod_{k\in F_{n,d}} \phi_{k,n,\gamma}$ where $\phi_{k,n,\gamma}$ is grouping all factors of order k. The purpose of this note is to clarify the calculation of the polynomials $\phi_{k,n,\gamma}$ by induction.

2. DEFINITION OF $\psi_{k,\alpha}$

Let p be a prime integer, n an integer coprime with p and $\alpha \in \mathbb{F}_p^*$.
Let ξ be a primitive k-root i.e. ξ is in the group $\left(\overline{\mathbb{F}_p}\right)^*$ and has order k. As $(\mathbb{F}_p)^*$ is a subgroup of $\left(\overline{\mathbb{F}_p}\right)^*$ we can consider the morphism $\mathbb{Z} \to \left(\overline{\mathbb{F}_p}\right)^* / (\mathbb{F}_p)^*$ defined by $s \mapsto \xi^s$. This morphism has a kernel of type $r\mathbb{Z}$ with $r = \inf\{s \in \mathbb{N}^* \,|\, \xi^s \in (\mathbb{F}_p)^*\}$. As a result $\xi^r = \alpha \in (\mathbb{F}_p)^*$. Moreover, as ξ has order k, we can easily see that $r\text{ord}(\alpha) = k$. Let l_k be defined by $l_k = \gcd(k, p-1)$. We prove now that $\text{ord}(\alpha) = l_k$: we have $\text{ord}(\alpha) \mid p-1$ because $\alpha \in (\mathbb{F}_p)^*$, and we have $\text{ord}(\alpha) \mid k$, so $\text{ord}(\alpha) \mid l_k$ hence $\text{ord}(\alpha) \leq l_k$. In order to show $l_k \leq \text{ord}(\alpha)$, as $\text{ord}(\alpha) = \frac{k}{r}$ we have $l_k \leq \text{ord}(\alpha) \iff l_k \leq \frac{k}{r} \iff r \leq \frac{k}{l_k}$. To prove the last inequality it suffices to show that $\xi^{k/l_k} \in (\mathbb{F}_p)^*$ because in that case, from the definition of r, we will have $r \mid \frac{k}{l_k}$. It is the case because $\left(\xi^{k/l_k}\right)^{l_k} = 1$ hence $\text{ord}\left(\xi^{k/l_k}\right) \mid l_k$ so $\text{ord}\left(\xi^{k/l_k}\right) \mid p-1$ and hence $\xi^{k/l_k} \in (\mathbb{F}_p)^*$. As a result $r = \frac{k}{l_k}$ and r only depends on k (and not on ξ): let us denote it r_k and we have $k = r_k l_k$. The following proposition sums up the above paragraph.

Proposition 1. *Let $k \neq 0$ be an integer. Let $l_k = \gcd(k, p-1)$ and $r_k = \frac{k}{l_k}$. Let ξ be a k-primitive root of $\overline{\mathbb{F}_p}$. Then we have*

$$r_k = \inf\{s \in \mathbb{N}^* \,|\, \xi^s \in (\mathbb{F}_p)^*\},$$
$$\xi^{r_k} = \alpha \in (\mathbb{F}_p)^* \text{ and } \text{ord}(\alpha) = l_k.$$

We can now introduce the definition of the polynomial $\psi_{k,\alpha}$.

Definition 1. *For all integer $k \neq 0$, let $l_k = \gcd(k, p-1)$ and $r_k = \dfrac{k}{l_k}$. For all α l_k-th primitive root, we define the polynomial $\psi_{k,\alpha}$ to be the product of all the irreducible factors of the cyclotomic polynomial ϕ_k whose roots ξ verify $\xi^{r_k} = \alpha$ (if a root verify that, all the roots verify that too because they are conjugated via Frobenius).*

In conjunction with proposition 1, the above definition gives the following proposition.

Proposition 2. *Let $k \in \mathbb{N}^*$, l_k and r_k as defined above. With notation P^k for the set of primitive k-roots,*

1. *for all $\alpha \in P^{l_k}$, $\psi_{k,\alpha}$ divides $X^{r_k} - \alpha$,*
2. *$\phi_k = \prod_{\alpha \in P^{l_k}} \psi_{k,\alpha}$ and hence for all $\alpha \in P^{l_k}$, $\deg(\psi_{k,\alpha}) = \frac{\varphi(k)}{\varphi(l_k)}$,*
3. *for all $\alpha \in P^{l_k}$, the polynomial $\psi_{k,\alpha}$ is irreducible if and only if*
$$\varphi(l_k) \times \mathrm{ord}_{\mathbb{Z}_p^*}(p) = \varphi(k).$$

Let us prove the first point: the fact that $\psi_{k,\alpha} \mid X^{r_k} - \alpha$ is a direct consequence of the definition of $\psi_{k,\alpha}$. The second point is a direct result of proposition 1 and the calculation of the degree is then the consequence of the following facts: there are $\varphi(l_k)$ l_k-primitive roots denoted $\alpha_1, \ldots, \alpha_{\varphi(l_k)}$, all the ψ_{k,α_i} have same degree (from [1]) and ϕ_k has degree $\varphi(k)$. The third point comes from the well-known fact that the minimal polynomials ϕ_ξ of $\xi \in P^k$ are of degree the order $\mathrm{ord}_{\mathbb{Z}_k^*}(p)$ of p in the group $\mathbb{Z}_k^*$.

3. Application to factorization of $X^n - \gamma$

3.1. **Indistinguishability of irreducible factors of $\psi_{k,\alpha}$.** Let n be an integer and $\gamma \in (\mathbb{F}_p)^*$ of order d. Let us remark firstly that for all k-primitive root ξ we have $\phi_\xi \mid X^n - \gamma$ if and only if $\xi^n = \gamma$. In such a case, with $r = r_k$, we have from proposition 1 $r_k \mid n$ and $\gamma = \xi^n = (\xi^{r_k})^{n/r_k} = \alpha^{n/r}$. So by denoting P^k the k-th primitive roots and $P^k_\alpha = \{\zeta \in P^k \,|\, \zeta^{r_k} = \alpha\}$, for all $\zeta \in P^k_\alpha$ we have $\zeta^n = (\zeta^r)^{n/r} = \alpha^{n/r} = \gamma$ so $\phi_\zeta \mid X^n - \gamma$. As a result we can conclude that $\psi_{k,\alpha} \mid X^n - \gamma$. The following proposition sums up the above paragraph.

Proposition 3. *Let $n \in \mathbb{N}^*$, $\gamma \in (\mathbb{F}_p)^*$. For all $k \in \mathbb{N}^*$ and $\alpha \in (\mathbb{F}_p)^*$, denoting*
$$P^k_\alpha = \{\xi \in P^k \,|\, \xi^{r_k} = \alpha\}$$
we have

1. *for all $\xi \in P^k_\alpha$, if $\phi_\xi \mid X^n - \gamma$ then $\psi_{k,\alpha} \mid X^n - \gamma$,*
2. *$\psi_{k,\alpha} \mid X^n - \gamma$ if and only if $r_k \mid n$ and $\alpha^{n/r_k} = \gamma$.*

From the first point of this proposition we could say that the family of polynomials $(X^n - \gamma)_{n \in \mathbb{N}, \gamma \in \mathbb{F}_p^*}$ doesn't distinguish or doesn't separate the irreducible factors of the $\psi_{k,\alpha}$.

3.2. **Factorization by order grouping of $X^n - \gamma$.** Let us search now the factorization of $X^n - \gamma$ as expected in the introduction. We have seen in [1] that the polynomials $X^n - \gamma$ for $\gamma \in (\mathbb{F}_p)^*$ have for irreducible factors the irreducible factors of ϕ_k for $k \in \mathrm{Div}(nd) \setminus \bigcup_{l|d,\ l \neq d} \mathrm{Div}(nl)$ (recalling that $d = \mathrm{ord}(\gamma)$). From the first subsection above we can deduce that the polynomial $X^n - \gamma$ have as factors polynomials of type $\psi_{k,\alpha}$ for $k \in \mathrm{Div}(nd) \setminus \bigcup_{l|d,\ l \neq d} \mathrm{Div}(nl)$. But from proposition 3 we have $\psi_{k,\alpha} \mid X^n - \gamma$ if and only if $r_k \mid n$ and $\alpha^{n/r_k} = \gamma$. As a result, denoting $F_{n,d} = \mathrm{Div}(nd) \setminus \bigcup_{l|d,\ l \neq d} \mathrm{Div}(nl)$, we have

$$X^n - \gamma = \prod_{\substack{k \in F_{n,d} \\ r_k | n \\ \alpha^{n/r_k} = \gamma}} \psi_{k,\alpha} \tag{1}$$

Let us remark that from [1], we know that if $k \in F_{n,d}$ then there exists α such that $\psi_{k,\alpha} | X^n - \gamma$. As a result the condition $r_k \mid n$ is superfluous, and so we can write

$$X^n - \gamma = \prod_{\substack{k \in F_{n,d} \\ \alpha^{n/r_k} = \gamma}} \psi_{k,\alpha}$$

Let us remark that there might exist an order k with $r_k \mid n$ without $\psi_{k,\alpha} \mid X^n - \gamma$ because for all α of order l_k we will never have $\alpha^{n/r_k} = \gamma$.
Finally, we can prove that among the three conditions under the product of equation 1 we can remove the condition $k \in F_{n,d}$: let us consider (k, α) such that $r_k \mid n$ and $\alpha^{n/r_k} = \gamma$. First of all, for all $\xi \in P_\alpha^k$, $\xi^{nd} = (\xi^r)^{\frac{n}{r}d} = \alpha^{\frac{n}{r}d} = \gamma^d = 1$ so $k \mid nd$. Next $\operatorname{ord}(\alpha^{n/r_k}) = \operatorname{ord}(\gamma)$, but as $\operatorname{ord}(\alpha^{n/r_k}) = l_k / \gcd\left(\frac{n}{r_k}, l_k\right)$ (recalling that $\operatorname{ord}(\alpha) = l_k$) then $l_k = d \times \gcd\left(\frac{n}{r_k}, l_k\right) = \gcd\left(\frac{nd}{r_k}, l_k d\right)$. As $k = r_k l_k$ then $l_k = \gcd\left(\frac{nd}{k} l_k, d l_k\right) = \gcd\left(\frac{nd}{k}, d\right) l_k$ and hence $\gcd\left(\frac{nd}{k}, d\right) = 1$ i.e. $\frac{nd}{k}$ is coprime to d. This imply directly that $k \notin \bigcup_{l|d,\ l \neq d} \operatorname{Div}(nl)$: else $nl = km$ with $d = lf$ and $f \neq 1$ hence $nd = kfm$ and $\frac{nd}{k} = fm$ is so not coprime with d. So we get the below theorem.

Theorem 1. *Let n be an integer, $\gamma \in (\mathbb{F}_p)^*$, then denoting*

$$F_{n,d} = \operatorname{Div}(nd) \setminus \bigcup_{l|d,\ l \neq d} \operatorname{Div}(nl)$$

we have

$$X^n - \gamma = \prod_{\substack{k \in F_{n,d} \\ \alpha^{n/r_k} = \gamma}} \psi_{k,\alpha} = \prod_{\substack{r_k | n \\ \alpha^{n/r_k} = \gamma}} \psi_{k,\alpha}.$$

4. Example

Let us compute by induction the polynomials $\psi_{k,\alpha}$ and the factorizations of some polynomials $X^n - \gamma$ in $\mathbb{F}_7$. The order of elements of $(\mathbb{F}_7)^* = (\mathbb{Z}/7\mathbb{Z}) \setminus \{0\}$ are given in the following table.

element	1	2	3	4	5	6
order	1	3	6	3	6	2

Let us now compute the polynomials $\psi_{k,\alpha}$ for various k.

- For the order $k = 1$ we have $l_1 = \gcd(1, 6) = 1$ so $\alpha = 1$ and $r_1 = 1$ hence $\psi_{1,1} = \phi_1 = X - 1$.
- For the order $k = 2$ we have $l_2 = \gcd(2, 6) = 2$ so $\alpha = 6$ and $r_2 = 1$ hence $\psi_{2,6} = \phi_2 = X - 6$.
- For the order $k = 3$ we have $l_3 = \gcd(3, 6) = 3$ so $\alpha \in \{2, 4\}$ and $r_3 = 1$ hence $\psi_{3,2} = X - 2$ and $\psi_{3,4} = X - 4$.
- For the order $k = 4$ we have $l_4 = \gcd(4, 6) = 2$ so $\alpha = 6$ and $r_4 = 2$ hence $\psi_{4,6} = \phi_4$ divides $X^2 - 6$. But $\deg(\phi_4) = \varphi(4) = 2$ so $\psi_{4,6} = X^2 - 6$.
- For the order $k = 5$ we have $l_5 = \gcd(5, 6) = 1$ so $\alpha = 1$ and $r_5 = 5$ hence $\psi_{5,1} = \phi_5$ divides $X^5 - 1$. But $X^5 - 1 = \phi_5 \phi_1 = \phi_5 \times (X - 1)$ so $\phi_5 = \frac{X^5 - 1}{X - 1} = 1 + X + X^2 + X^3 + X^4$.
- For the order $k = 6$ we have $l_6 = \gcd(6, 6) = 6$ so $\alpha \in \{3, 5\}$ and $r_6 = 1$ hence $\psi_{6,3} = X - 3$ and $\psi_{6,5} = X - 5$.
- For the order $k = 7$ we have $l_7 = \gcd(7, 6) = 1$ so $\alpha = 1$ and $r_7 = 7$ hence as in the case $k = 5$ we have $\psi_{7,1} = \phi_7 = 1 + X + \ldots + X^6$.

- For the order $k = 8$ we have $l_8 = \gcd(8, 6) = 2$ so $\alpha = 6$ and $r_6 = 4$ hence $\psi_{8,6} = \phi_8$ divides $X^4 - 6$. But $\deg(\phi_8) = \varphi(8) = 4$ so $\psi_{4,6} = X^4 - 6$.
- For the order $k = 9$ we have $l_9 = \gcd(9, 6) = 3$ so $\alpha \in \{2, 4\}$ and $r_9 = 3$ hence $\psi_{9,2} \mid X^3 - 2$ and $\psi_{9,4} \mid X^3 - 4$. But $\psi_{9,2}$ and $\psi_{9,4}$ have same degree and multiplied give ϕ_9 which has degree $\varphi(9) = 6$ so they both have degree 3. As a result $\psi_{9,2} = X^3 - 2$ and $\psi_{9,4} = X^3 - 4$.
- For the order $k = 10$ we have $l_{10} = \gcd(10, 6) = 2$ so $\alpha = 6$ and $r_{10} = 5$ hence $\psi_{10,6} = \phi_{10}$ divides $X^5 - 6$. But as $F_{5,2} = \mathrm{Div}(10) \setminus \mathrm{Div}(5) = \{10, 2\}$ then $X^5 - 6 = \phi_{10}\phi_2 = \phi_{10} \times (X + 1)$ so by euclidean division we get $\psi_{10,6} = X^4 - X^3 + X^2 - X + 1$.
- For the order $k = 11$ we have $l_{11} = \gcd(11, 6) = 1$ so $\alpha = 1$ and $r_{11} = 11$ hence as in case $k = 5$ we get $\phi_{11,1} = 1 + X + \ldots + X^{10}$.
- For the order $k = 12$ we have $l_{12} = \gcd(12, 6) = 6$ so $\alpha \in \{3, 5\}$ and $r_{12} = 2$ hence $\psi_{12,3} \mid X^2 - 3$ and $\psi_{12,5} \mid X^2 - 5$. As in case $k = 9$ we have $\deg(\psi_{12,\alpha}) = \frac{\varphi(12)}{2} = 2$ so $\psi_{12,3} = X^2 - 3$ and $\psi_{12,5} = X^2 - 5$.
- For the order $k = 13$ we have $l_{13} = \gcd(13, 6) = 1$ so $\alpha = 1$ and $r_{13} = 13$ hence as in case $k = 5$ we get $\phi_{13,1} = \phi_{13} = 1 + X + \ldots + X^{12}$.
- For the order $k = 14$ we have $l_{14} = \gcd(14, 6) = 2$ so $\alpha = 6$ and $r_{14} = 7$ hence $\psi_{14,6} = \phi_{14}$ divides $X^7 - 6$. But as $F_{7,2} = \mathrm{Div}(14) \setminus \mathrm{Div}(7) = \{14, 2\}$ then $X^7 - 6 = \phi_{14}\phi_2 = \phi_{14} \times (X + 1)$ so by euclidean division we get $\psi_{14,6} = X^6 - X^5 + \ldots - X + 1$.
- For the order $k = 15$ we have $l_{15} = \gcd(15, 6) = 3$ so $\alpha \in \{2, 4\}$ and $r_{15} = 5$ hence $\psi_{15,2} \mid X^5 - 2$ and $\psi_{15,4} \mid X^5 - 4$. But $F_{5,3} = \mathrm{Div}(15) \setminus \mathrm{Div}(5) = \{15, 3\}$ then $X^5 - 2 = \psi_{15,2}\psi_{3,4}$ (because $4^{15/3} = 2$) and $X^5 - 4 = \psi_{15,4}\psi_{3,2}$ (because $2^{15/3} = 4$). As a result
$$\psi_{15,2} = \frac{X^5 - 2}{X - 4} = X^4 + 4X^3 + 2X^2 + X + 4$$
$$\psi_{15,4} = \frac{X^5 - 4}{X - 2} = X^4 + 2X^3 + 4X^2 + X + 2$$

References

[1] Gabriel Soranzo. "Factorisation of $X^n - \alpha$ over finite fields". In: (July 2022). DOI: 10.5281/zenodo.6789183. URL: https://doi.org/10.5281/zenodo.6789183.

Email address: gabriel.soranzo@u-pec.fr